JTN 2015
Universidad de Valladolid
June 29-July 3, 2015

Applications of the Generalization of the Theorem of Proth to primality Test of Generalized Fermat Numbers

Pedro Berrizbeitia[1], Thomas G. Berry[2], Daniel Sadornil[3], Juan Tena-Ayuso[4]

[1] *Universidad Simón Bolívar, Caracas, Venezuela, pberrizbeitia@gmail.com*
[2] *Universidad Simón Bolívar, Caracas, Venezuela, berrytgk@gmail.com*
[3] *Universidad de Cantabria, Santander, España, sadornild@unican.es*
[4] *Universidad de Valladolid, Valladolid, España, juantenaayuso@gmail.com*

Abstract

We give fast deterministic primality test for, $F_{k,t} = (2k)^{2^t} + 1$, for $k = 1, 3, 5$ and 17, and for all $t \geq 1$.

For $k = 1$ we give minor improvements of the celebrated Pepin Test for Fermat primes. For $k = 3$ we give a test that improves slightly the test naturally derived from [1], as well as the test described in [4]. For $k = 5$ the test improves the test described in [3] as well as the one described in [4]. For $k = 17$ the test is a clear improvement of the test derived from [2], and implemented in [5].

1 extended abstract

Modern primality tests begin when Lucas in 1876 gave his test for primality Mersenne numbers $2^p - 1$:

Theorem 1. If p is an odd prime, and $M_p = 2^p - 1$, then the following are equivalent:

1. M_p is prime.
2. $(-2+\sqrt{3})^{2^{p-1}} \equiv -1 \pmod{M_p}$.
3. The sequence defined by $S_0 = 4$; $S_{k+1} = S_k^2 - 2$, for $k \geq 0$, satisfies $S_{p-2} \equiv 0 \pmod{M_p}$.

The famous Lucas-Lehmer test is stated as the equivalence of items (1) and (3) in Theorem 1 above.

The "impressive" computational feature of the test is summarized as follows: *The primality of M_p is determined by computing $p-2$ modular squares (squares of integers modulo M_p), where modular additions are neglected.* Item (2) shows that the primality of M_p can be determined by that the computation of $(-2+\sqrt{3})^{M_p} \pmod{M_p Z[\sqrt{3}]}$, where the congruence occurs in the ring $Z[\sqrt{3}]$. We refer to such congruence as a Fermat type congruence.

The Theorem extends to what we call the Lucasian Test, that is, a deterministic test for $n = A \cdot 2^s - 1$, $s \geq 2$ and $A < 2^s$, provided that $d \in Z$, and $\alpha \in Z[\sqrt{d}]$ are given, such that $(\frac{d}{n}) = -1 = (\frac{\alpha\sigma(\alpha)}{n})$, where $(\frac{\cdot}{n})$ is the Jacobi symbol and $\sigma(\alpha)$ is the Galois conjugate of α in the ring $Z[\sqrt{d}]$.

The celebrated 1878 Theorem of Proth (or Proth Test) is an efficient primality test for all numbers of the form $n = A \cdot 2^s + 1$, $s \geq 2$ and $A < 2^s$.

The Theorem of Proth states that if n satisfies the hypothesis above and $a \in Z$ is given such that $(\frac{a}{n}) = -1$ is given, then

$$n \text{ is prime if, and only if, } a^{\frac{n-1}{2}} \equiv -1 \pmod{n}.$$

Both, The Proth and the Lucasian tests, require of an integer a so that the Jacobi Symbol $(\frac{a}{n}) = -1$. Such a can be found usually very quickly by using the Quadratic Reciprocity Law (QRL), so the Proth Test and Lucasian Tests are considered as applications of QRL to primality testing. The tests are particularly efficient when A is small, and the famous Pepin Test for Fermat Numbers is a particular instance of this theorem of Proth when $A = 1$.

For small values of A, both Test the primality of n after performing almost exactly $\log_2 n$ modular multiplications.

Hugh Williams and collaborators, in a series of papers beginning in the 70's, extended Lucas's methods to arbitrary primes p and gave many concrete algorithms; an overview of this work can be found in Williams's book [5]. The number of modular multiplications is $O(\log n)$ if A is bounded, but the implied constant grows notably with A.

In [2], three of the authors of the present work used general properties of the power residue symbol in cyclotomic fields, including the general Eisenstein's Reciprocity Law, to generalize Proth Test and apply it to determining primality of many numbers $n = Am^s + \omega_s$, where $s \geq 2$, $A < m^s$, ω_s may be ± 1, or be roots of 1 mod m^s, of order dividing $\phi(m)$, where ϕ is the Euler-phi function. Their result improves on the methods used Williams and collaborators in many respects. We state the main theorem in [2]:

Theorem 2. Suppose $n = A \cdot m^s + \omega_s$; $s \geq 2$; $A < m^s$; $\omega_s < m^s$; $n^f \equiv 1 \pmod{m^s}$, where $f = ord_m(n)$ is the order of f mod m. Suppose further that if $x^{\phi(m)} \equiv 1 \pmod{m^s}$ and $1 < x < m^s$ then x does not divide n. Let $a \in Z[\zeta_m]$ such that the m-th power residue symbol $(\frac{a}{n})_m$ is a primitive m-th root of 1. Then the following are equivalent:

1. n is prime.
2. $(a^{\tau\gamma})^{\frac{n^{\phi(f)}-1}{m}} \equiv (\frac{a}{n})_m \pmod{nZ}[\zeta_m]$, where τ and γ are specific elements of the group ring $Z[Gal(Q[\zeta_m]/Q)]$ given in [2] and $\phi(k)$ is the Euler Phi function.
3. same as item (2) except that the congruence holds modulo an Ideal ν of the cyclotomic ring $Z[\zeta_m]$ lying over $nZ[\zeta_m]$.

Note that this general theorem is very much like the original Proth or even the Lucasian theorem in that the primality of certain type of natural numbers n can be determined with only one Fermat type computation. The main "computational problem" is that according to item (2) the congruence modulo n occurs in the m-th Cyclotomic Ring, which has of degree $\phi(m)$ over the ring of rational integers Z, so the number of modular multiplications required is multiplied by a factor of around $O(\phi(m)^2)$. Recently, the autors of [5] describe an implementation of the test based on item (2) of Theorem 2. Equations in page 12 of [5] explicitly describe part of the implementation of the test for $m = 7$. To see them will give the reader an idea of how the difficulties of the implementation grow with m, as well as the complexity of the test. The authors In [2] mentioned that when possible (3) should be used instead of (2) and even announced a sequel to the paper where this was to be illustrated. In particular note that in the case $f = 1$, if the factorization of the ideal n is obtained, then the equation modulo the divisor ν of n turns into a Fermat type congruence in the Ring of Rational Integers, so the complexity will in fact be determined by the factorization of n rather than the computation of the congruence modulo ν.

The objective of the present paper is to achieve such sequel, for which we chose a family of numbers in which (3) can be used instead of (2). Such family also should have proven to be of interest in the literature. This is why we chose some Generalized Fermat numbers. They fit nicely the criteria.

The occasion of the "VI Jornadas de Teoría de Números" to be celebrated in Valladolid in June of this year was also not a random choice, but a way of celebrating and honoring the academic activity of Professor Juan Tena

Ayuso, in occasion of his retirement from the University of Valladolid, and of given a nice closure to this chapter of collaboration between the University of Valladolid in Valladolid, Spain and the University Simón Bolívar in Caracas, Venezuela, initiated towards the end of last century.

Hence we describe the test for $F_{k,t} = (2k)^{2^t} + 1$, for $k = 1, 3, 5$ and 17, and for all $t \geq 1$, mainly because those are cases where finding the ideal factorization for $F_{k,n}$ in the m-th cyclotomic ring is deterministic and possible to describe clearly, and also because an element a that depends only on k, but not on t, can be obtained from the k-th Eisenstein Reciprocity Law in the Cyclotomic Ring $Z[\zeta_k]$.

References

[1] Berrizbeitia, P.; Berry, T. G. *Cubic reciprocity and generalised Lucas-Lehmer tests for primality of* $A \cdot 3^n \pm 1$. Proc. Amer. Math. Soc. 127 (1999), no. 7, 1923–1925.

[2] Berrizbeitia, P.; Berry, T. G.; Tena-Ayuso, J. *A generalization of Proth's theorem.* Acta Arith. 110 (2003), no. 2, 107–115.

[3] Berrizbeitia, P.; Odremán, M.; Tena-Ayuso, J; *Primality test for numbers M with a large power of* 5 *dividing* $M^4 - 1$. Theoret. Comput. Sci. 297 (2003), no. 1-3, 25–36.

[4] H.C. Williams; *A note on the primality of* $6^{2^n} + 1$ *and* $10^{2^n} + 1$, The Fibonacci Quarterly, 26(1988), 296Ð305.

[5] Y Yingpu Deng, Chang Lv; *Primality Test for Numbers of the Form* $Ap^n + w_n$ arXiv:1306.4562 [math.NT]